UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,412	01/02/2004	Ryo Ochi	247305US6	2841

22850 7590 03/15/2010

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
03/15/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/749,412	OCHI ET AL.	
	Examiner	Art Unit	
	CANH LE	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-16 and 18-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-16 and 18-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the communication filed on 11/19/2009.

Claims 7 and 17 have been cancelled.

Claims 1-6, 8-16, and 18-22 have been amended.

Claims 1-6, 8-16, and 18-22 have been examined and are pending.

Response to Arguments

Applicant's arguments, see page 14, filed 11/19/2009, with respect to the objection of claims 2-6, 10, 12-16, and 20 have been fully considered. The objection of claims 2-6, 10, 12-16, and 20 has been withdrawn due to amendment.

Applicant's arguments, see page 16, filed 11/19/2009, with respect to the specification have been fully considered. The objection of the specification has been withdrawn due to amendment.

Applicant's arguments, see pages 15-16, filed 11/19/2009, with respect to the 35 U.S.C. § 112, 1st rejection of claims 1-6, 8-16, and 18-22 have been fully considered. The 35 U.S.C. § 112, 1st rejection of claims 1-6, 8-16, and 18-22 has been withdrawn due amendment.

Applicant's arguments, see page 16, filed 11/19/2009, with respect to the 35 U.S.C. § 112, 2nd rejection of claims 1-6, 8-16, and 18-22 have been fully considered. The 35 U.S.C. §112, 2nd rejection of claims 1, 9, 11, 19, and 21-22 has been withdrawn due to amendment.

Applicant's arguments, see pages 16-17, filed 11/19/2009, with respect to the 35 U.S.C. § 101 rejection of claims 1-6, 8-16, and 18-20 have been fully considered. The 35 U.S.C. § 101 rejection of claims 1-6, 8-16, and 18-20 has been withdrawn due to amendment.

Applicant's arguments filed 11/19/2009 have been fully considered but they are not persuasive.

The Applicant argues the following:

(a) Claim 1 patentably distinguishes over Schneier and Lin, either alone or in proper combination; Lin does not disclose or suggest "said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group," according to a "first group" and a "second group" which are defined in amended Claim 1.

The Examiner respectfully disagrees for the following reasons:

Per (a): The combination of Schneier and Lin teach the amended claim 1.

Schneier teaches dividing, at the encryption processing apparatus, an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data *[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES]* setting, at the

encryption processing apparatus, a mixed encryption processing sequence by mixing processing sequences of encryption processing units of the plurality of groups with each other *[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining encryption]* executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from another the second group and under a condition in which a processing sequence of the encryption processing units, set in said dividing, within each group is fixed *[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs]* but does explicitly disclose the input data is different for a first group and second group and the input data to be encrypted for the first group is generated independently relative to the input data to be encrypted for the second group.

Lin teaches encryption system resists differential power analysis attacks wherein inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups and an input data of the encrypting processing unit is independent with a first group of the groups *[Lin: pg. 11; Insert "dummy" S block look-ups in to the DES routine, lines 10-28; Inserting Insert "dummy" S block is known as the second*

group. The input data for the second group (i.e. of Lin) is different for a first group of the groups (i.e. of Schneier). An input data is encryption for the second group which is generated independently relative to the input data to be encrypted for the first group of Schneier].

It would have been obvious to one of ordinary skill in the art at the time of the invention was make to combine the Schneier and Lin inventions, and have "inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups and an input data of the encrypting processing unit is independent with a first group of the groups", as taught by Lin, thereby it would perform the DES operation and the benefit gained in DPA attack resistance , as discussed by Lin, [Lin: pg. 11, lines 18-19].

Therefore, the combination of Schneier and Lin positively teach the claim limitation.

Claim Objections

Claims 9 and 20-21 are objected to because of the following informalities: Appropriate correction is required.

Claim 9 recites the limitation "from another one of the groups" should be replaced by "from the second group" to be consistent with other language of independent claims (i.e. claims 1, 11, 19, and 21-22).

Claim 21-22 recite "A *computer readable storage medium*;" Although, the publication specification recites "recording medium" such as CD-ROM, DVD, a magnetic disk. However, Broadly interpreted, a "computer readable storage medium" can be any means that include propagate and transmission signals, which are non-eligible subject matter user 35 U.S.C. 101.

The Examiner respectfully suggests that the claims be amended as "A *non-transitory computer readable storage medium*" and the specification to include *non-transitory* to make the claim statutory under 35 U.S.C. 101.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-6, 8-16, and 18-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "wherein ***the input data*** to be encrypted for *a first group* of the groups is ***different relative to the input data*** to be encrypted for *a second group* of the groups, and ***the input data*** to be encrypted for the first group is generated independently relative to ***the input data*** to be encrypted for the second group" in lines 8-11 (emphasis added). It is unclear how "***the input data*** to be encrypted for *a first group* of the groups is ***different relative to the input data*** to be encrypted for *a second group* of the groups. It is unclear how the meaning of "***the input data***" in the phrase of "***the input data*** to be encrypted for *a first group* of the groups" and "***the input data"*** in the phrase "***the input data*** to be encrypted for *a second group* of the groups" is different while it refers to the same ***"the input data"***. For the purpose of applying prior art, the Examiner interprets the aforementioned as two separate inputs (i.e. a *first input data*

to be encrypted for a first group of the groups and *a second input data to be encrypted for a second group of the groups).*

Similarly, claims 9, 11, 19, and 21-22 recites the limitation "wherein ***the input data*** to be encrypted for *a first group* of the groups is ***different relative to the input data*** to be encrypted for *a second group* of the groups, and ***the input data*** to be encrypted for the first group is generated independently relative to ***the input data*** to be encrypted for the second group" (emphasis added). It is unclear how "***the input data*** to be encrypted for *a first group* of the groups is ***different relative to the input data*** to be encrypted for *a second group* of the groups. It is unclear how the meaning of "***the input data***" in the phrase of "***the input data*** to be encrypted for *a first group* of the groups" and "***the input data"*** in the phrase "***the input data*** to be encrypted for *a second group* of the groups" is different while it refers to the same ***"the input data"***. For the purpose of applying prior art, the Examiner interprets the aforementioned as two separate inputs (i.e. a *first input data to be encrypted for a first group of the groups* and *a second input data to be encrypted for a second group of the groups).*

Claims 2-6, 8, 10, 12-16, 18 and 20 are rejected due virtual dependency of claims 1, 9, 11, and 19 respectively.

The Examiner kindly requests the Applicant to point out and explain with specificity (i.e. column and line) in the specification where it describes/supports the aforementioned limitation (Emphasis added).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 9-15, 19, and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruce Schneier,** "Applied Cryptography", 2nd edition, John Wiley & Son, pg. 265-279, pg. 357-263, 1996 in view of **Bo Lin et al.** (GB 2 345 229 A) and further in view of

As per claims 11, 1, 21:

Claim 11:

Schneier teaches an encryption processing method, implemented on an encryption processing apparatus, for performing a data encryption process, said encryption processing method comprising:

(a) dividing, at the encryption processing apparatus, an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block**

Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES], [[where the input data to be encrypted for a first group of the groups is different relative to the input data to be encrypted for a second group of the groups, and the input data to be encrypted for the first group is generated independently relative to the input data to be encrypted for the second group]];

(b) setting, at the encryption processing apparatus, a mixed encryption processing sequence by mixing processing sequences of encryption processing units of the plurality of groups with each other **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining encryption]** executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from another the second group and under a condition in which a processing sequence of the encryption processing units, set in said dividing, within each group is fixed **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs]**; and

(c) performing, at the encryption processing apparatus, an encryption process in accordance with the mixed encryption processing sequence set in said setting **[Schneier: pg.**

358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; Triple-DES Cipher Block Chaining encryption is build on 3 DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining (TCBC) encryption. The TCBC includes a triple-DES encryption process].

Schneier does not explicitly disclose the input data is different for a first group and second group; the input data to be encrypted for the first group is generated independently relative to the input data to be encrypted for the second group.

However, attention is directed to Lin, which teaches encryption system resists differential power analysis attacks wherein inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups and an input data of the encrypting processing unit is independent with a first group of the groups **[Lin: pg. 11; Insert "dummy" S block look-ups in to the DES routine, lines 10-28; Inserting Insert "dummy" S block is known as the second group. The input data for the second group (i.e. of Lin) is different for a first group of the groups (i.e. of Schneier). An input data is encryption for the second group which is generated independently relative to the input data to be encrypted for the first group of Schneier].**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was make to combine the Schneier and Lin inventions, and have "inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups and an input data of the encrypting processing unit is independent with a first group of the groups", as taught by Lin, thereby it would perform the DES operation and the benefit gained in DPA attack resistance , as discussed by Lin, **[Lin: pg. 11, lines 18-19].**

Claims 1 and 21 are essentially the same as claim 11 except that they set forth the claimed invention as an apparatus / a computer readable storage medium rather than a method and rejected under the same reasons as applied above.

As per claims 12, 2:

Claim 12:

The combination of Schneier and Lin teach the subject matter as described above.

Schneier further teaches the encryption processing method according to Claim 11, wherein each group includes a triple-DES encryption process **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES].**

Lin further teaches, setting a dummy encryption processing unit that performs the dummy encryption process in at least one of the groups, and setting the mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing said dummy encryption processing unit **[Lin: abstract, pg. 11, lines 10-28; "Another technique which could be used to improve resistance to attacks is to *insert* "dummy" operation to confuse analysis of a power signature… The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance …". It would have been obvious for setting the number of single-**

DES processes of dummies to be set to a multiple of 3 corresponding to the triple DES because each number of single-DES is set to 1].

dividing includes setting a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups, and setting the number of single-DES processes of dummies to be set to a multiple of 3 **[Lin: abstract, pg. 11, lines 10-28; "Another technique which could be used to improve resistance to attacks is to insert "dummy" operation to confuse analysis of a power signature… The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance …". It would have been obvious for setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple DES because each number of single-DES is set to 1].**

Claim 2 is essentially the same as claim 12 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claim 13, 3:

Claim 13:

The combination of Schneier and Lin teach the subject matter as described above.

Schneier further teaches the encryption processing method according to Claim 11, wherein said dividing determines a group of sequences, which can be performed independently of each other, within the original encryption processing sequence to be divided in a process of

division into the plurality of groups, and performs a process for setting a group of divisions in which each of the sequences in the group of sequences can be performed independently as a unit **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DES; page 272, figure 12.2 One round of DES; Each S-box independently performs an encryption processing as a unit]**.

Claim 3 is essentially the same as claim 13 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 14, 4:

Claim 14:

The combination of Schneier and Lin teach the subject matter as described above.

Schneier further teaches the encryption processing method according to Claim 11, wherein each of said encryption processing units is a single-DES encryption process,

(a) said dividing divides the original encryption processing sequence containing one or more single-DES encryption processes into a plurality of groups composed of one or more single-DES encryption processes **[Schneier : pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs]**, and

(b) said setting sets one mixed encryption processing sequence by mixing the single-DES encryption processing units contained in each group by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed **[Schneier : pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; Triple-DES Cipher Block Chaining encryption is build on 3 DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining encryption. Each triple-DES is fixed]**.

Claim 4 is essentially the same as claim 14 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 15, 5:

Claim 15:

The combination of Schneier and Lin teach the subject matter as described above.

Schneier further teaches the encryption processing method according to Claim 11, wherein

said dividing performs a process for dividing the encryption processing sequence into a plurality of groups composed of one or more encryption processing units with a single-DES encryption process which forms a triple-DES encryption process being an encryption processing unit **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher**

Block Chaining encryption is build on 3 DESs].

Claim 5 is essentially the same as claim 15 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 19, 9, 22:

Claim 19:

Schneier teaches an encryption processing method, implemented on an encryption processing apparatus, for performing a data encryption process, said encryption processing method comprising:

(a) dividing, at the encryption processing apparatus, an original encryption processing sequence, into a plurality of groups, each group being composed of a plurality of encryption processing units **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs]**, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data **[Schneier: pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES]**, [[where the input data to be encrypted for a first group of the groups is different relative to the input data to be encrypted for a second group of the groups, and the input data to be encrypted for the first

group is generated independently relative to the input data to be encrypted for the second group]];

(b) setting, at the encryption processing apparatus, a mixed encryption processing sequence [**Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining encryption]** [[by adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence]] and by mixing processing sequences of the encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group [**Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; Inner CBC and outer CBC modes; Each triple-DES is fixed**]; and

(c) performing, at the encryption processing apparatus, an encryption process in accordance with said mixed encryption processing sequence [**Schneier : pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; Triple-DES Cipher Block**

Chaining encryption is build on 3 DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining (TCBC) encryption. In the TCBC includes a triple-DES encryption process].

Scheier does not explicitly disclose adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence.

However, Lin teaches encryption system resists differential power analysis attacks wherein adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence **[Lin: abstract, pg. 11, lines 10-28; "Another technique which could be used to improve resistance to attacks is *to insert* "dummy" operation to confuse analysis of a power signature… The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance…"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the encryption processing method of Schneier by including the teaching of Lin because it would perform the DES operation and the benefit gained in DPA attack resistance **[Lin: pg. 11, lines 18-19].**

Claims 9 and 22 are essentially the same as claim 19 except that they set forth the claimed invention as an apparatus / a computer readable storage medium rather than a method and rejected under the same reasons as applied above.

As per claims 20, 10:

Claim 20:

Schneier and Lin teach the subject matter as described above.

Schneier further teaches the encryption processing, wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process **[Schneier : pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs]**,

Lin further teaches said dummy encryption processes as a single-DES encryption process **[Lin: abstract, pg. 11, lines 10-28"; "Another technique which could be used to improve resistance to attacks is to insert "dummy" operation to confuse analysis of a power signature… The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance…"]**, and

Schneier and Lin do not explicitly disclose wherein said dividing includes setting the number of dummy encryption processes to a multiple of 3.

It would have been obvious for setting the number of single-DES processes of dummies

to be set to a multiple of 3 corresponding to the triple DES because each number of single-DES is set to 1.

Claim 10 is essentially the same as claim 20 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Claims 6 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruce Schneier,** "Applied Cryptography", 2nd edition, John Wiley & Son, pg. 265-279, pg. 357-263, 1996 in view of **Bo Lin et al.** (GB 2 345 229 A) further in view of **Kocher et al.** (US 2001/0053220 A1).

As per claims 16, 6:

Claim 16:

The combination of Schneier and Lin teach the subject matter as described above.

Schneier and Lin do not explicitly disclose in details a random-number generation process as a process including a conversion process by three single-DES processes and setting the three single-DES processes as a random- number generation process in one of the groups.

However, Kocher teaches a random-number generation process as a process including a conversion process by three single-DES processes and setting the three single-DES processes as a random-number generation process in one of the groups **[Kocher: par. [0006]; "triple DES (a cipher constructed using three applications of Data Encryption Standard using different keys) can resist all feasible cryptanalytic attacks, provided that attackers only have access**

to the standard inputs to and outputs from the protocol"; par. [0008], lines 6-8; a key management devices introduce randomness].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the encryption processing method of Schneier and Lin by including the teaching of Kocher because it would provide unpredictability into their internal state **[Kocher, par. [008]].**

Claim 6 is essentially the same as claim 16 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Claims 8 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruce Schneier,** "Applied Cryptography", 2nd edition, John Wiley & Son, pg. 265-279, pg. 357-263, 1996 in view of **Bo Lin et al.** (GB 2 345 229 A) further in view of **Kaminaga et al** (US 2002/0124179 A1).

As per claims 18, 8:

Claim 18:

The combination of Schneier and Lin teach the subject matter as described above.

Schneier and Lin do not explicitly disclose in details storing processing results in a memory for storing processing results of the encryption processing units which form the mixed

encryption processing sequence in such a manner as to be capable of identifying which encryption processing unit the processing results are obtained from.

However, Kaminaga teaches storing processing results in a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence to identify which encryption processing unit the processing results are obtained from **[Kaminaga: abstract, par. [0039], lines 7-10; "processed by an encryption process (step 503). The result Z obtained in the process performed in step 503 is stored on a RAM (step 504)"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the encryption processing method of Schneier and Lin by including the teaching of Kaminaga because it would detect an erroneous operation during encryption processing is that before the output of the encrypted result, the ciphertext result, the ciphertext is again decrypted to a plaintext and compared with the original text, and when they are identical to each other, the ciphertext is output and when they are different, the result of the encryption-process is not output to the external device **[Kaminaga, par. [0014]].**

Claim 8 is essentially the same as claim 18 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Conclusion

The examiner requests, in response to this Office action, support be shown for language added to any original claims on amendment and any new claims. That is, indicate support for

newly added claim language by specifically pointing to page(s) and line number(s) in the specification and/or drawing figure(s). This will assist the examiner in prosecuting the application. Failure to show support can result in a non-compliant response.

When responding to this office action, Applicant is advised that if Applicant traverses an obviousness rejection under 35 U.S.C. 103, a reasoned statement must be included explaining why the Applicant believes the Office has erred substantively as to the factual findings or the conclusion of obviousness See 37 CFR 1.111(b).

Additionally Applicant is further advised to clearly point out the patentable novelty which he or she thinks the claims present, in view of the state of the art disclosed by the references cited or the objections made. He or she must also show how the amendments avoid such references or objections See 37 CFR 1.111(c).

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Orgad Edan can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

March 8, 2010

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439